WHAT IS CLAIMED IS:

1. A method of enabling access to a resource of a processing system, comprising the steps of:

establishing a secure communication session between a user desiring access and a logon component of the processing system;

verifying that logon information, provided by the user to the logon component during the secure communication session, matches stored information identifying the user to the processing system;

generating a security context from the logon information and authorization information that is necessary for access to the resource;

providing the security context to the user; and

sending, by the user to the processing system, the security context and a request for access to the resource.

2. The method of claim 1, wherein the resource is at least one of a processor, a program object, and a record of the processing system.

3. The method of claim 1, wherein the logon component provides a symmetric encryption key to the user in establishing the secure communication session.

4. The method of claim 1, wherein the logon information includes a password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position.

5. The method of claim 4, wherein the logon information is verified by checking for agreement between the stored information identifying the user to the processing system and the password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position provided by the user to the logon component.

6. The method of claim 1, wherein the security context comprises a plaintext header and an encrypted body, and the plaintext header comprises a security context ID, a key handle, and an algorithm identifier and key size.

7. The method of claim 6, wherein the encrypted body comprises at least one of a user identifier, an organization identifier, access information, an expiration time, public key information, symmetric key information, and a hash.

8. The method of claim 7, wherein the access information specifies at least one resource accessible by the user; the expiration time specifies a time after which the security context is

invalid; the hash is computed over the plaintext header and the encrypted body before encryption; and the hash is digitally signed by the logon component.

9. The method of claim 7, wherein the encrypted body includes the expiration time and access to the resource is denied if the expiration time differs from a selected time.

10. The method of claim 1, further comprising the step of determining, by a stateless component of the processing system, based on the security context sent with the request for access by the user, whether access to the requested resource should be granted to the user.

11. The method of claim 10, wherein the request for access is at least partially encrypted with a symmetric encryption key extracted from the security context.

12. The method of claim 11, wherein a hash value is computed over the request for access, the hash value is included with the security context and the request for access sent by the user to the processing system, the integrity of the request for access is checked based on the hash value, and access is granted only if the integrity of the hash value is verified.

13. The method of claim 10, wherein the user digitally signs the request for access, the user's digital signature is included with the security context and the request for access sent by the user to the processing system, the user's digital signature is checked by the processing system, and access to the resource is granted only if the user's digital signature is authenticated.

14. The method of claim 13, wherein the request for access comprises a wrapper.

15. The method of claim 10, further comprising the step, after access to the requested resource is granted, of sending a response to the user that includes a request counter that enables the user to match the response to the request for access.

16. The method of claim 1, wherein at least one of a client time and a request counter is sent by the user to the processing system with the security context and the request for access to the resource.

17. The method of claim 16, wherein the request counter is sent by the user and access to the resource is denied if the request counter differs from a predetermined value.

18. A method of accessing a resource of a processing system, comprising the steps of:

providing by a user logon information to a logon component of the processing system during a secure communication session between the user and the processing system;

verifying that the provided logon information matches stored information identifying the user to the processing system;

generating a security context from the logon information and authorization information that is necessary for access to the resource, wherein the security context comprises a plaintext

header and an encrypted body; the plaintext header comprises a security context ID, a key handle, and an algorithm identifier and key size; and the encrypted body comprises at least one of a user identifier, an organization identifier, access information, an expiration time, public key information, symmetric key information, and a hash;

providing the security context to the user;

sending, by the user to the processing system, the security context and a request for access to the resource; and

determining, by a stateless component of the processing system, based on the security context sent with the request for access by the user, whether access to the requested resource should be granted to the user.

19. The method of claim 18, wherein the security context includes a symmetric encryption key, and the request for access is at least partially encrypted with the symmetric encryption key.

20. The method of claim 18, wherein the logon information includes a password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position.

21. The method of claim 20, wherein the logon information is verified by checking for agreement between the stored information identifying the user to the processing system and the password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position provided by the user to the logon component.

22. The method of claim 18, wherein the access information specifies at least one resource accessible by the user; the expiration time specifies a time after which the security context is invalid; the hash is computed over the plaintext header and the encrypted body before encryption; and the hash is digitally signed by the logon component.

23. The method of claim 18, wherein the encrypted body includes the expiration time and access to the resource is denied if the expiration time differs from a selected time.

24. The method of claim 18, wherein a hash value is computed over the request for access, the hash value is included with the security context and the request for access sent by the user to the processing system, the integrity of the request for access is checked based on the hash value, and access is granted only if the integrity of the hash value is verified.

25. The method of claim 18, wherein the user digitally signs the request for access, at least the user's digital signature and the request for access are enclosed in a wrapper, the security

context and the wrapper are sent to the processing system, the user's digital signature is checked by the processing system, and access to the resource is granted only if the user's digital signature is authenticated.

26. The method of claim 18, further comprising the step, after access to the requested resource is granted, of sending a response to the user that includes a request counter that enables the user to match the response to the request for access.

27. The method of claim 18, wherein at least one of a client time and a request counter is sent by the user to the processing system with the security context and the request for access to the resource.

28. The method of claim 27, wherein the request counter is sent by the user and access to the resource is denied if the request counter differs from a predetermined value.

29. A processing system having resources that are selectively accessible to users, the resources including processors, program objects, and records, the processing system comprising:

a communication device through which a user desiring access to a resource communicates sends and receives information in a secure communication session with the processing system;

an information database that stores information identifying users to the processing system and authorization information that identifies resources accessible to users and that is necessary for access to resources; and

a logon component that communicates with the communication device and with the information database, wherein the logon component receives logon information provided by the user during the secure communication session, verifies the received logon information by matching against information identifying the user to the processing system that is retrieved from the information database, and generates a security context from the received logon information and authorization information;

wherein the logon component provides the security context to the user's communication device, and the user sends, to the processing system, the security context and a request for access to a resource.

30. The processing system of claim 29, further comprising a cryptographic accelerator, and wherein the logon component receives a symmetric encryption key from the cryptographic accelerator and provides the symmetric encryption key to the user's communication device.

31. The processing system of claim 29, wherein the logon information includes a password and at least one of a user identifier, an organization identifier, a sub-organization

identifier, a user location, a user role, and a user position.

32. The processing system of claim 31, wherein the logon component verifies received logon information by checking for agreement between information identifying the user to the processing system that is retrieved from the information database and the password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position provided by the user to the logon component.

33. The processing system of claim 29, wherein the security context comprises a plaintext header and an encrypted body, and the plaintext header comprises a security context ID, a key handle, and an algorithm identifier and key size.

34. The processing system of claim 33, wherein the encrypted body comprises at least one of a user identifier, an organization identifier, access information, an expiration time, public key information, symmetric key information, and a hash.

35. The processing system of claim 34, wherein the access information specifies at least one resource accessible by the user; the expiration time specifies a time after which the security context is invalid; the hash is computed over the plaintext header and the encrypted body before encryption; and the hash is digitally signed by the logon component.

36. The processing system of claim 34, wherein the encrypted body includes the expiration time and access to the resource is denied if the expiration time differs from a selected time.

37. The processing system of claim 29, further comprising a stateless component that determines, based on the security context sent with the request for access by the user, whether access to the requested resource should be granted to the user.

38. The processing system of claim 37, wherein the communication device at least partially encrypts the request for access with a symmetric encryption key included in the security context.

39. The processing system of claim 38, wherein a hash value is computed over the request for access, the hash value is included with the security context and the request for access sent by the user to the processing system, the integrity of the request for access is checked based on the hash value, and access is granted only if the integrity of the hash value is verified.

40. The processing system of claim 37, wherein the communication device appends a digital signature of the user to the request for access, at least the user's digital signature and the request for access are enclosed in a wrapper, the security context and the wrapper are sent to the processing system, the logon component checks the user's digital signature, and access to the

resource is granted only if the user's digital signature is authenticated.

41. The processing system of claim 37, wherein after access to the requested resource is granted, the stateless component sends a response to the user that includes a request counter that enables the user to match the response to the request for access.